REMARKS

The present Amendment cancels claims 8, 9, 11-13, and adds new claims 14-18. Therefore, the present application has pending claims 14-18.

Interview Summary

Applicants thank the Examiner for granting the interview conducted on July 25, 2007. In the interview, the Examiner recommended amending the claims to more clearly describe features of the present invention. The Examiner also directed Applicants' attention to U.S. Patent No. 6,678,827 to Rothermel et al. ("Rothermel"), which the Examiner previously made of record, but did not rely upon. In this response, Applicants have amended the claims in accordance with the Examiner's recommendations. Applicants will contact the Examiner to further discuss the claims, as now more clearly recited.

35 U.S.C. §112 Rejections

Claims 11 and 12 stand rejected under 35 U.S.C. §112, second paragraph as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. As previously discussed, claims 11 and 12 were canceled. Therefore, this rejection regarding claims 11 and 12 is rendered moot.

35 U.S.C. §102 Rejections

Claims 8, 9, 11 and 13 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,484,261 to Wiegel. As previously

discussed, claims 8, 9, 11 and 13 were canceled. Therefore, this rejection regarding claims 8, 9, 11 and 13 is rendered moot.

35 U.S.C. §103 Rejections

Claim 12 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Wiegel in view of CERT's CC Vendor-Initiated Bulletins 1994-1998. As previously discussed, claim 12 was canceled. Therefore, this rejection regarding claim 12 is rendered moot.

New Claims 14-18

Claims 14-17 were added to more clearly describe features of the present invention. Specifically, claims 14-18 more clearly recite that the present invention is directed to a security management method and system as recited, for example, in independent claims 14 and 18.

The present invention, as recited in claim 14, and as similarly recited in claim 18, provides a security management method for supporting security management of a plurality of managed systems executed in an information system, where the information system includes computers connected through a network. The method includes designing security specifications to be applied to the information system by using an information security policy designated by a user. According to the present invention, the information security policy is applied to each of the plurality of managed systems designated by the user. Also according to the present invention, the information security policy is selected from a first database, which includes a correspondence between information security policies and security measures.

Furthermore, according to the present invention, each security measure indicates an action to be taken to secure the managed systems. The method also includes auditing a security status of the information system with respect to the information security policy designated by the user, where the security status indicates whether a security measure has been executed. In addition, the method includes changing the security status of each of the managed systems based on a result of auditing the security status. The method also includes auditing the security status of the information system every time a security setting is changed. The prior art does not disclose all of these features.

The above described features of the present invention, as now more clearly recited in the claims, are not taught or suggested by any of the references of record, particularly Wiegel, whether taken individually or in combination with any of the other references of record.

Wiegel teaches a method of managing graphical network security policy. However, there is no teaching or suggestion in Wiegel of the security management method and system as recited in claims 14 and 18 of the present invention.

Wiegel discloses a method of establishing a representation of an abstract network security policy. The representation is established in the form of a decision tree that is constructed by assembling graphical symbols representing policy actions and policy conditions. A user modifies properties of the graphical symbols to create a logical representation of the policy.

Concurrently, the logical representation is transformed into a textual script that represents the policy, and the script is displayed as the user works with the logical representation. When the policy representation is saved, the script is translated into machine instructions that govern the operation of a network gateway or firewall. The policy representation is named. The policy representation may be applied to other network devices or objects by moving an icon identifying the representation over an icon representing the network device. Policies, network objects, and network services are stored in the form of trees.

One feature of the present invention, as recited in claim 14, and as similarly recited in claim 18, includes designing security specifications to be applied to the information system by using an information security policy designated by a user, where the information security policy is applied to each of the plurality of managed systems designated by the user, where the information security policy is selected from a first database, which includes a correspondence between information security policies and security measures, and where each security measure indicates an action to be taken to secure the managed systems. To further illustrate this feature, the Examiner's attention is directed to Fig. 5 of the present application, which shows the contents of an information security policy database 132. Column 51 describes an identifier POLICYID for uniquely identifying an information security policy. Column 52 describes measure categories of the information security policy described in the space of the POLICYID of column 51. The

measure categories include, for example, an identification and authentication function, and an access control function. Column 53 describes a security measure, which expresses the contents of the information security policy described in the space of the POLICYID 51. The security measure includes, for example, a limitation of a terminal capable of accessing the network, and an execution of a good password establishment for identification and authentication information. Wiegel does not disclose this feature.

For example, Wiegel does not disclose a first database that includes a correspondence between information security policies and security measures, where each security measure indicates an action to be taken to secure the managed systems, as in the present invention. As described, for example, in column 15, lines 43-67, Wiegel merely describes security policies that are available for application to nodes of a network. As shown in Fig. 3, the policy tree 316 has top-level nodes named Internet Policies and My Policies. The Internet Policies include a policy named "E-mail, Web, and FTP." The name of this policy indicates that it establishes security rules for use of Internet e-mail, World Wide Web, and FTP services. This is not the same as the present invention.

Another feature of the present invention, as recited in claim 14, and as similarly recited in claim 18, includes auditing a security status of the information system with respect to the information security policy designated by the user, where the security status indicates whether a security measure has been executed. To further illustrate this feature of the present invention,

the Examiner's attention is directed to Fig. 19. As shown, column 73 describes security information for the system to be audited by the audit program. The security information includes: the existence of the execution of the security measure, which can be specified by the information security policy database 132, the security measure being represented by the information policy specified by POLICY ID 61, which corresponds to the audit program in the security management and audit program database 133 shown in Fig. 6; and the security status 732 regarding the security measure of the system. The security status 732 refers, for example, to setting information that relates to a connection of the router to an external network when the security measure is "a limitation of terminals able to access to an external network" and when the system to be audited is "router". Wiegel does not disclose this feature.

For example, as described in column 11, lines 38-41, Wiegel discloses where the system may include a monitor agent that is responsible for monitoring, reporting, and notification about the security status of the other agents that surround the knowledge base 202. Wiegel is silent as to what the security status represents.

Yet another feature of the present invention, as recited in claim 14, and as similarly recited in claim 18, includes auditing the security status of the information system every time a security setting is changed. Wiegel does not disclose this feature. As previously discussed, Wiegel is silent as to what security status represents. Therefore, it follows that Wiegel does not teach or

suggest auditing the security status of the information system every time a security setting is changed.

Therefore, Wiegel fails to teach or suggest "designing security specifications to be applied to the information system by using an information security policy designated by a user, wherein the information security policy is applied to each of the plurality of managed systems designated by the user, wherein the information security policy is selected from a first database, which includes a correspondence between information security policies and security measures, and wherein each security measure indicates an action to be taken to secure the managed systems" as recited in claim 14, and as similarly recited in claim 18.

Furthermore, Wiegel fails to teach or suggest "auditing a security status of the information system with respect to the information security policy designated by the user, wherein the security status indicates whether a security measure has been executed" as recited in claim 14, and as similarly recited in claim 18.

Further, Wiegel fails to teach or suggest "auditing the security status of the information system every time a security setting is changed" as recited in claim 14, and as similarly recited in claim 18.

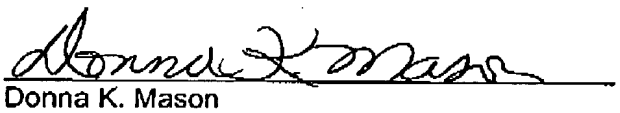
Therefore, Wiegel does not teach or suggest the features of the present invention, as recited in claims 14-18. Accordingly, claims 14-18 are not anticipated by Wiegel.

In view of the foregoing amendments and remarks, Applicants submit that claims 14-18 are in condition for allowance. Accordingly, early allowance of claims 14-18 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (566.39530VX1).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Donna K. Mason
Registration No. 45,962

DKM/cmd
(703) 684-1120